

System Management for the new Enterprise environment

Belarc, Inc.
Two Clock Tower Place, S. 520
Maynard, MA 01754 USA
Tel: (+1) 978-461-1100
Web: <http://www.belarc.com>

Enterprises today are becoming more geographically distributed, are adding ever more computer systems and are placing new demands on their IT staffs, because of security, corporate governance and compliance requirements[†]. These requirements are in addition to traditional IT management tasks such as software license compliance, hardware refreshes, patching, software deployment, lifecycle management and others.

Because of this new environment, traditional system management suites may not be the best approach for the Enterprise. Historically, IT system management architectures have focused on either managing the main-

[†]. **Sarbanes-Oxley Act of 2002**, requires U.S. public companies to follow new guidelines for corporate governance and financial accountability.

FISMA requires all U.S. Federal Agencies and the DoD to implement an IT security process as specified by NIST (National Institute of Standards and Technology).

HIPAA focuses on the safeguarding of electronic protected health information and applies to Health Care Providers, Health Plans and Health Care Clearinghouses.

FFIEC is an Interagency body which proscribes uniform standards for the Federal examination of U.S. financial institutions, including IT security compliance.

frames or the local networks, either LANs or more recently Domains. Management systems for mainframes, such as IBM's Tivoli or CA's Unicenter, are excellent for this purpose, but are not well suited for managing systems on many distributed LANs or Domains. Microsoft's SMS was designed for managing systems on individual LANs and Domains. However, all of these management suites require a complex hierarchy of servers, replication of databases and much manual labor to implement and maintain. This paper recommends that Enterprise IT management consider an entirely new architecture to help manage certain aspects of their IT systems.

The case for an IT Portal architecture

Most large Enterprises are finding that their Intranet networks are indispensable to their operations and communications. Many applications that were originally designed to run on client-server environments have been, or are being, re-written to run in a native Intranet environment. This can and should also be true for IT management applications. An IT Portal system running in a native Intranet environment can offer the Enterprise significant benefits in automation and savings in manpower and costs.

Some examples of the benefits of an IT Portal architecture are outlined below.

IT Security

Software security patches and updates will continue to be a major requirement and expense for all Enterprises. When a request goes out to the local administrators to implement a security patch, does management have an independent verification that this was accomplished, and when? Do the local administrators know which systems require the patches and which patches were not successfully installed? An IT Portal based management system could automatically answer these questions for both management and local administrators.

In addition to software patches and updates, IT security managers should also be aware of their system configurations and whether they meet established security benchmarks[†]. Up until now, these benchmarks have been primarily applied to critical enterprise servers, however the threats and attacks on the enterprise's desktops and laptops is equally real. For details, please ask for our white paper, "*Security Within - Configuration based Security*".

Software License and Version Control

Enterprises need to have a software license compliance process in place which accurately reflects their use of licensed software but does not require them to over-pay software vendors. Related to this is the need to know the versions of the software installed, for both COTS and custom built applications, and the installation of prohibited software, such as file sharing and spyware programs.

To meet these requirements using traditional client-server based management suites requires an enormous amount of manpower and time. It is not unusual for an Enterprise to have over 30,000 unique software signatures to maintain, with new ones coming in daily. Even after this effort has been made, the results are often out of date and do not accurately reflect the large number of software changes happening daily.

An IT Portal based management system can automate the entire software discovery process using a single server and database for the entire Enterprise, and this information can be updated on a daily basis. See the case studies listed in the “Proof Positive” section below. In addition there is no longer a need to maintain software signatures to accomplish these objectives.

Corporate Governance and Compliance

Most enterprises are impacted by the corporate governance requirements of Sarbanes-Oxley and may also be impacted by the IT security compliance requirements of either HIPAA, FISMA or the FFIEC. Satisfying these regulations requires the CIO, CISO and sometimes the CEO to certify that their IT systems have the proper level of security[†]. However in all cases the actual work of accomplishing these tasks is dependent on many local administrators.

[†]. Setting and monitoring configurations based on consensus benchmarks is important to IT security because it is a pro-active way to avoid many successful attacks. The U.S. National Security Agency has found that configuring computers with proper security settings blocks over 90% of the existing threats. (IA Newsletters “Security Benchmarks: A Gold Standard.” [Click here](#) to request a copy.)

[†]. These regulations typically define IT Security as a process consisting of identifying the IT systems in the enterprise; assigning a risk category to these systems based on the risk of loss of Confidentiality, Integrity and Availability; running controls or benchmarks against these systems based on their risk category; correcting for deficiencies; and continually monitoring the controls on these systems.

In order for the CIO and CISO to have confidence to sign on the dotted line, they should have independent verification that the tasks were accomplished in the proper manner. Also, many local administrators will need guidance on how to implement these regulations, and IT management should have the ability to see the current status of these compliance tasks across the Enterprise. An IT Portal architecture is ideal to satisfy the requirements in all of these cases. For more information, please request our white paper, “[*Automating the FISMA Process*](#)”.

Managing the Outsourcer

Outsourcing IT functions is becoming more common for modern Enterprises. This may be done for specified routine tasks or in some cases such as the NMCI[†] contract, outsourcing the complete management and control of the network and IT infrastructure. In all cases where IT outsourcers are used for more than routine tasks, management should have a way of independently verifying that the tasks were accomplished, or the systems maintained at the contracted level.

It makes little sense to have detailed service levels specified in the contract, without also having a way to independently verify that these service levels were achieved. An IT Portal based system which requires little or no maintenance is an excellent way to implement an independent monitoring system for outsourced contracts. For more information about this, please request our white paper, “[*IT as a Utility - Recommendations for Success*](#)”.

Working as a team

Large geographically distributed Enterprises usually have an equally distributed IT organization consisting of local administrators, and regional and headquarters management. Usually these different groups in the IT organization are not making decisions based on the same data. When management requests reports based on Enterprise wide data, it puts an added burden on the local and regional administrators. What is needed is a much more automated system, which spans the entire Enterprise network.

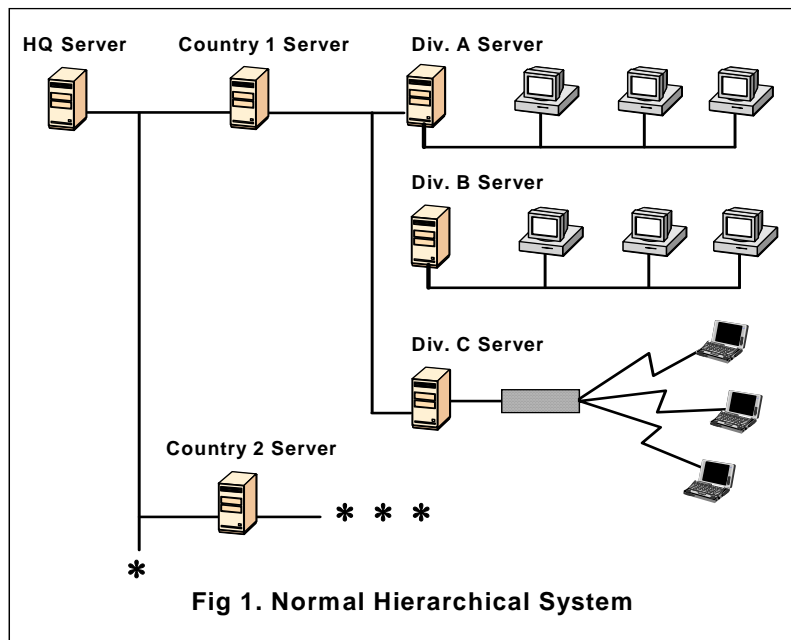
Local administrators don’t need to “own” the IT management system. They do need to have easy access to its functions. Headquarters personnel should have access to up-to-date Enterprise wide data, without plac-

[†]. Navy Marine Corps Intranet is the largest U.S. Federal government IT contract, and is managed by EDS.

ing extra burdens on the local administrators. This can all be accomplished with an IT Portal architecture.

IT Portal Architecture

Traditional management systems have hierarchical architectures, like the one shown in Fig 1.

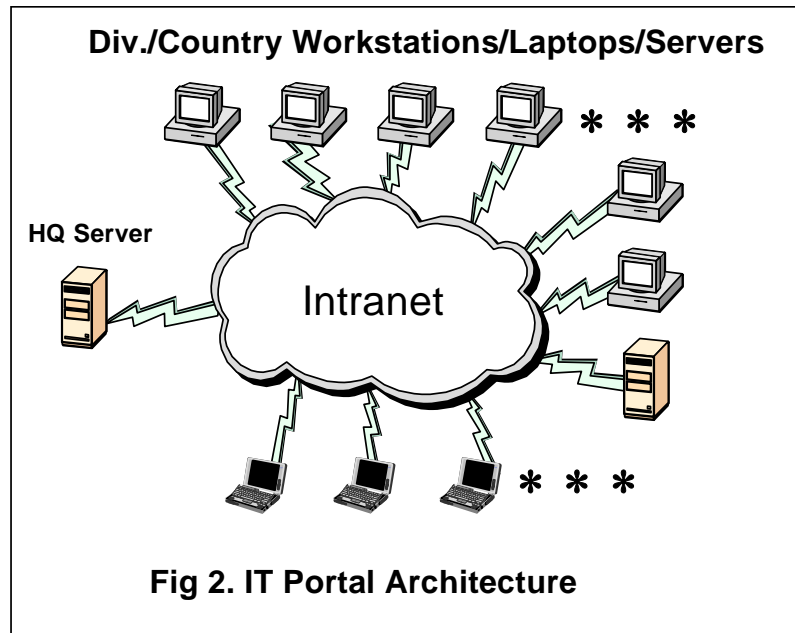


These hierarchical systems require separate servers and databases for each LAN or Domain. In order for this information to be available to headquarters IT personnel, these databases are required to be replicated and synchronized at the next level in the hierarchy and eventually reside on a corporate HQ server. Remote systems create further complications since they require additional and special remote access servers.

IT Portal Architecture

In contrast, an IT Portal architecture is based on lightweight agents which use the Enterprise's Intranet and requires only one server and a single database (see Fig 2).

This architecture allows for easy deployment and little if any local administration. The agents run as a "service" and therefore do not need a user to be logged on to the computer to operate. Unconnected machines,



such as remote machines and laptops, will automatically upload the next time they connect to the network.

This architecture also allows for easy sharing and access to the information by both local administrators and regional and headquarters management. Web based reports can be automatically created based on the user's login, so that each user will see information relevant to their area of responsibility. For additional information, please request our white paper, "[System Management for the Internet Age](#)".

Proof Positive

Belarc's products all incorporate the IT Portal architecture and these products have been successfully used by large Enterprise customers for the past four years. Brief descriptions of three of our customers are below.

Dana Corporation

Dana is a Fortune 200 global auto parts manufacturer and has a very decentralized organization. They have over 25,000 desktops, servers and laptops in 30 countries around the world, which send daily updates to their BelManage server. Over 300 local administrators log into their BelManage system to see the status of their computer assets. Dana's IT orga-

nization uses BelManage on a regular basis for software license control, software and hardware upgrade planning, and PC life-cycle planning. The BelManage database is also linked to Dana's on-line purchase requisition and ordering system. For additional information, [click here](#)

U.S. Marine Corps

The USMC has deployed BelManage across their entire world-wide network of over 90,000 computers, including servers, desktops and laptops. BelManage runs on a single W2000 server and Oracle database in Quantico, VA, and the profiles are updated daily. The system is accessed by hundreds of remote administrators throughout the world. The HQ IT staff uses BelManage for security audits, software application consolidation, hardware upgrade planning, server consolidation, and day-to-day management of their computer assets. For additional information, [click here](#):

U.S. National Park Service

The Park Service deployed BelManage across their entire network of 22,000 computer assets in two weeks time. These computers are located from Alaska to the Everglades, often in very remote areas. The Park Service uses BelManage for security audits, software application consolidation, hardware upgrade planning, software license control, and more. For additional information, [click here](#):

Summary

IT managers in today's Enterprise are faced with many new requirements, such as IT security, corporate governance and compliance, managing outsourcers, and all the while trying to run an efficient IT organization with large numbers of geographically distributed IT assets. The traditional IT management suites were not designed to meet these requirements and do not operate easily in this environment. The IT Portal architecture helps the Enterprise to meet these requirements by automating many of these steps and using the Enterprise's existing Intranet network. Belarc offers a proven IT Portal architecture as the best way to address the needs of today's Enterprise.

Contact Us:

For additional information and a briefing of our capabilities, please contact us.

Belarc, Inc.

Two Clock Tower Place, Suite 520

Maynard, MA 01754 USA

Tel: (+1) 978-461-1100

Email: info@belarc.com

Web: <http://www.belarc.com>

Copyright © 2005 Belarc, Inc. All rights reserved. Belarc, BelManage and BelSecure are registered trademarks or trademarks of Belarc, Inc. All other trademarks mentioned in this document are the property of their respective owners.